SISTEM APLIKASI KRIPTOGRAPHY ADVANCED ENCRYPTION STANDARD

Laporan Penelitian

Disusun oleh:

Heri Santoso, M.Kom

NIDN. 0119116701

PROGRAM STUDI ILMU KOMPUTER

FAKULTAS SAINS DAN TEKNOLOGI

UIN SUMATERA UTARA MEDAN

2017

LEMBAR PENGESAHAN

Judul Penelitian	**SISTEM APLIKASI RIPTOGRAPHY ADVANCED ENCRYPTION STANDARD**
Bidang Ilmu	: Teknologi Informatika
Topik Unggulan	: Komputasi
Ketua Peneliti	
a. Nama Lengkap	: Heri Santoso, M.Kom
b. NIDN	: 0119116701
c. Jabatan Fungsional /	: Asisten Ahli
d. Fakultas/Jurusan	: Fakultas Sains dan Teknologi
e. Pusat Penelitian	: Prodi Ilmu Komputer
f. Alamat Institusi	: Kampus 1 UIN Sumatera Utara Medan
g. Telpon/Faks/E-mail	: Jln. IAIN No.1, Medan 20235
	: 082167005000 / Herisantoso@uinsu.ac.id
h. Lama Penelitian Keseluruhan	: 3 Bulan
i. Biaya Penelitian yang dihabiskan	: Dana mandiri Rp. 3.000.000,-

Medan, September 2017

Mengetahui,

Kaprodi Ilmu Komputer

Ketua Peneliti,

Mhd Furqan, S.Si., M.Comp.Sc.
NIDN. 2006078003

Heri Santoso, M.Kom
NIDN. 0119116701

KATA PENGANTAR

Segala puji bagi Allah SWT yang senantiasa memberikan taburan rahmat dan karunia-NYA sehingga penulis dapat menyelesaikan laporan penelitian yang berjudul : *"***SISTEM APLIKASI KRIPTOGRAPHY ADVANCED ENCRYPTION STANDARD*".***

Penulisan Laporan Penelitian ini dilakukan dalam rangka melengkapi kewajiban menjadi seorang Dosen dalam melaksanakan Tri Dharma Perguruan Tinggi. Penulis menyadari sepenuhnya bahwa dalam penulisan Penelitian banyak pihak yang membantu dan berpartisipasi. Untuk itu ucapan terima kasih khususnya penulis ucapkan kepada :

1. Bapak Dr. H. M. Jamil, M.A selaku Dekan Fakultas Sains dan Teknologi UIN Sumatera Utara Medan.
2. Bapak Mhd Furqan, S.Si., M.Comp.Sc., selaku Ketua Program Studi Ilmu Komputer Fakultas Sains dan Teknologi UIN Sumatera Utara Medan
3. Teman-teman Dosen yang telah membantu pelaksanaan penelitian ini.
4. Teman-teman Staf Laboratorium yang turut membantu atas terselesaikannya penelitian ini.

Atas semua jasa tersebut, penulis serahkan kepada Allah SWT, semoga dibalas dengan Rahmat yang berlipat ganda. Walaupun Penelitian ini telah tersusun dengan sebaik mungkin, penulis tetap mengharapkan kritik dan saran yang membangun untuk penyempurnaan penelitian ini. Semoga penelitian ini dapat berguna bagi kita semua dan bagi penulis sendiri khususnya.

Medan, September 2017
Peneliti,

Heri Santoso, M.Kom

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

ABSTRAK

Citra digital merupakan salah satu data atau informasi yang sering disalahgunakan, oleh karena itu untuk menjaga keamanan dan kerahasiaan suatu data citra digital menjadi hal yang penting. Salah satu pengamanan bisa dilakukan dengan menerapkan algoritma Rijndael. Empat proses utama algoritma ini terdiri dari satu proses permutasi(*ShiftRows*) dan tiga proses subtitusi (*SubBytes*, *MixColumns*, dan *AddRoundKey*) dan juga proses penjadwalan kunci. Dalam penelitian ini akan dibahas tentang pengamanan citra digital dengan algoritma Rijndael dan juga implementasi algoritma ini dalam mengamankan citra digital. Algoritma Rijndael terdapat dalam proses enkripsi dan dekripsi yang dapat diaplikasikan untuk pengamanan citra digital. Hasil dari aplikasi ini mampu mengenkripsi dan mendekripsi *file* citra tanpa mengubah integritas data dari *file* citra tersebut.

Kata Kunci : Citra Digital, Algoritma Rijndael, Enkripsi, Dekripsi